# PATENT ABSTRACTS OF JAPAN

(11)Publication number:

2001-014796

(43)Date of publication of application: 19.01.2001

(51)Int.CI.

G11B 20/10 HO4N 5/91 7/08 HO4N 7/081 HO4N

(21)Application number: 11-233446

(71)Applicant: HITACHI LTD

(22)Date of filing:

20.08.1999

(72)Inventor: TAKAHASHI SUSUMU

TAKEUCHI TOSHIFUMI KAWAMAE OSAMU

(30)Priority

Priority number: 11121253

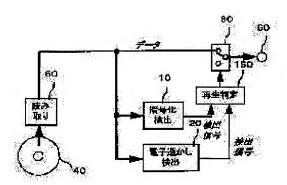
Priority date: 28.04.1999

Priority country: JP

### (54) REPRODUCING DEVICE AND DECODING DEVICE

## (57) Abstract:

PROBLEM TO BE SOLVED: To make it possible to surely reproduce a storage medium even though digital watermark information is detected erroneously concerning a normal storage medium enciphered through a predetermined cryptography. SOLUTION: Only in a non-ciphered case, a digital watermark is detected and reproduction is limited thereby. When an encryption detecting circuit 10 detects that a storage medium is not enciphered by a predetermined encipherment system and a digital watermark detector 20 detects digital watermark information, a reproduction limiting circuit 30 stops reproducing. When the encription detecting circuit 10 detects that the storage medium is enciphered by the predetermined encipherment system, the reproduction limiting circuit 30 does not stop reproducing.



会 8 (18) 日本国格群庁 (JP)

€ 摋 4 羋 华 噩

特開2001-14796 (11)特許出願公開番号

(P2001-14796A)

(43)公開日 平成13年1月19日(2001.1.19)

the second House I amount	デーヤコート。(参考)	H 5C053
The state of the s	FI	G11B 20/10

微別記号

5C063 5D044

5/91 7/08

7/08

5/91

G11B H04N (51) Int.Cl.7

H04N

(全9項) o L 審査請求 未酵水 請求項の数5

(21) 出版举号	<b>特顯平11-23344</b> 6	(71)出職人 000005108	000005108
			株式会社日立製作所
(22) 出願日	平成11年8月20日(1999.8.20)		東京都千代田区神田駿河台四丁目 6番地
		(72) 発明者	▲商▼橋 辞
(31) 優先権主張番号 特顯平11-121253	<b>特顯平11-121253</b>		神疾川県横浜市戸塚区吉田町292番地 株
(32)優先日	平成11年4月28日(1999.4.28)		式会社日立製作所デジタルメディア開発本
(33)優先権主張国	日本(JP)		都内
		(72) 発明者	竹内 散文
			神疾川県横浜市戸塚区吉田町292番地 株
			式会社日立製作所デジタルメディア開発本
			<b>第</b> 万
		(74)代理人	(74)代理人 100075096
			<b>弁理士 作田 康夫</b>
			最終買に続く

# 再生装置および復号装置 (54) [発明の名称]

<u>×</u>

【課題】電子透かしの誤検出によって所定の暗号方式で 暗号化された正規な蓄積媒体の再生も不可となってしま

とが検出され、電子透かし検出回路 (20) により電子 所定の暗号方式で暗号化されていることが検出された場 検出およびこれによる再生制限を行う。暗号化検出回路 (10) により所定の暗号方式で暗号化されていないこ による再生停止を行う。暗号化検出回路(10)により 【解決手段】暗号化されていない場合にのみ電子透かし 透かし情報が検出された場合に、再生制限回路(30) 合は、再生制限回路(30)は再生を停止しない。

関係の

、作許請求の範囲】

【請求項1】蓄積媒体に記録された映像または音声情報 を再生する再生装置において、 蓄積媒体に記録された映像または音声情報が所定の暗号 方式で暗号化されているかどうかを検出する暗号化検出 蓄積媒体に記録された映像または音声情報が所定の暗号 方式で暗号化されていない場合に映像または音声情報に 重畳されている少なくとも複製禁止を含む複製管理情報 を示す電子透かし情報を検出する電子透かし検出手段 蓄積媒体に記録された映像または音声情報が所定の暗号 方式で暗号化されていない場合には電子透かし検出手段

時に映像または音声情報の再生を停止する再生制限手段 の検出結果によって何らかの複製管理情報が検出された を有することを特徴とする再生装置。

映像または音声情報が電子透かし検出手段において電子 蓄積媒体に記録された映像または音声情報が所定の暗号 透かし情報を検出できるような正規な映像または音声情 **方式で暗号化されていない場合に蓄積媒体に記録された** 【請求項2】請求項1に記載の再生装置において、 報であるかどうかを解析する情報解析手段を有し、 蓄積媒体に記録された映像または音声情報が所定の暗号 方式で暗号化されていない場合に、情報解析手段によっ て電子透かし情報を検出できるような正規な映像または 音声情報ではないと判定された時にも、前記再生制限手 段は映像または音声情報の再生を停止することを特徴と

30 れ、これを復号して映像または音声情報を出力する復号 [請求項3] 符号化された映像または音声情報が入力さ

暗号化された入力符号化データを解読してもとの符号化 暗号解読手段を用いないで入力された符号化された映像 または音声情報を直接復号する場合に復号した映像また は音声情報に重畳されている少なくとも複製禁止を含む 複製管理情報を示す電子透かし情報を検出する電子透か された映像または音声情報を復元する暗号解読手段と、 し検出手段と、

または音声情報を直接復号する場合には、電子透かし検 映像または音声情報の出力を停止する出力制限手段を有 暗号解読手段を用いないで入力された符号化された映像 出手段によって何らかの複製管理情報が検出された時に することを特徴とする復号装置

複数の蓄積媒体の種類および蓄積媒体上の記録フォーマ ットを判別する媒体およびフォーマット判別手段を備 【請求項4】請求項1に記載の再生装置において、

暗号化検出手段は前記複数の蓄積媒体の種類および蓄積 媒体上の記録フォーマットそれぞれに定められた暗号方 式で暗号化されているかどうかを検出する手段であり、

特開2001-14796

ପ

びフォーマット判別手段で判別された蓄積媒体の種類お **t び蓄積媒体上の記録フォーマットで定められた暗号方** 式で暗号化されていない場合には、電子透かし検出手段 の検出結果によって何らかの複製管理情報が検出された 時に、再生制限手段は映像または音声情報の再生を停止 蓄積媒体に記録された映像または音声情報が、媒体およ することを特徴とする再生装置。

[請求項5] 符号化された映像または音声情報が入力さ れ、これを復号して映像または音声情報を出力する復号 被置において、 10 暗号化された入力符号化データを解読してもとの符号化 入力符号化データの供給装置との間の認証と暗号解読に された映像または音声情報を復元する暗号解読手段と、 必要なキー交換を行うAKE手段と

されている少なくとも複製禁止を含む複製管理情報を示 AKE手段で認証およびキー交換が成立しない状態で復 **号を開始した時に、復号した映像または音声情報に重疊** す電子透かし情報を検出する電子透かし検出手段と、 AKE手段で認証およびキー交換が成立しない状態で復 号を開始した時には、電子透かし検出手段によって何ら かの複製管理情報が検出された時に、映像または音声情 限の出力を停止する出力制限手段を有することを特徴と する復号装置。 20

[発明の詳細な説明]

E規に販売あるいは配布された蓄積媒体および正規に記 録された蓄積媒体は再生可能とし、違法に複製された媒 体は再生不可とする再生装置、および、正規に販売ある いは配布された蓄積媒体および正規に記録された蓄積媒 本から再生した符号は復号可能とし、遠法に複製された **媒体から再生した符号は復号不可とする復号装置に関す** 【発明の属する技術分野】本発明は著作権保護に関し、

[0002]

【従来の技術】ビデオディスク、ディジタルVTR、デ デオ信号に対する著作権保護を確実に行うようにしたど デオ信号処理装置や、ビデオ信号処理方法、記録媒体に 56号公報に記載されている。また、コピー防止のため = 0 x (NIKKEI ELECTRONICS 1998. 3. 23 (NO712) P47 ~ P5 イジタル放送の受信装置などにより得られる高画質のど 関する技術については、例えば、特開平10-1786 の認証とKEY交換については、例えば、日経エレクトロ 3) に記載されている。 40

**法に作成された蓄積媒体の再生を不可とする技術にまで** 育報を用いた複製防止技術が示されている。しかし、違 【発明が解決しようとする課題】前記公報には世代管理 は言及されていない。

[0004] 複製防止を確実に行うためには、暗号化の 技術が有効である。蓄積媒体に記録する映像または音声

-5-

20

1

€

[0005]しかし、暗号を解いて再生した映像または の電子透かしを検出して記録の制限を行ったり、再生し た映像または音声情報の電子透かしを検出して再生の制 限を行ったりして違法な複製および違法に複製された映 音声情報は自由に他の蓄積媒体に記録できてしまい、複 世代管理情報を映像または音声情報上に、視聴して も検知できない形で重畳する、いわゆる電子透かし技術 が有効である。すなわち、記録する映像または音声情報 製防止にならない。このような複製を防止するために 像または音声情報の視聴の防止に役立てることができ

術と電子透かし技術を併用した場合にどのようにして違 とにより、複製防止をより確実に行うことができる。す なわち、著作権を保護したい映像または音声情報には必 法に作成された蓄積媒体の再生を不可とするかについて 考慮されていなかった。特に、電子透かしの誤検出によ って正規に販売あるいは配布された蓄積媒体および正規 に記録された蓄積媒体の再生も不可となってしまう問題 【0006】暗号化技術と電子透かし技術を併用するこ ず電子透かしを付け、かつ蓄積媒体上では必ず暗号化す るようにすればよい。しかし、従来の技術は、暗号化技 について考慮されていなかった。

**債媒体については再生し視瞭することのできる様にした** 用した場合に、連法に作成された蓄積媒体については視 聴できないようにし、正規に作成され販売あるいは配布 された蓄積媒体、あるいは正規の方法に従い記録した蓄 技術、特に、電子透かしの誤検出によって正規に販売あ るいは配布された蓄積媒体および正規に記録された蓄積 媒体の再生および視聴も不可となってしまう問題を回避 する技術を示し、これらの技術を用いた再生装置および 【0007】本発明の目的は、暗号化と電子透かしを併 復号装置を提供することである。

検出手段と、蓄積媒体に記録された映像または音声情報 は音声情報に重畳されている少なくとも複製禁止を含む は、蓄積媒体に記録された映像または音声情報が所定の 暗号方式で暗号化されているかどうかを検出する暗号化 が所定の暗号方式で暗号化されていない場合に映像また 複製管理情報を示す電子透かし情報を検出する電子透か し検出手段と、蓄積媒体に記録された映像または音声情 報が所定の暗号方式で暗号化されていない場合には電子 透かし検出手段の検出結果によって何らかの複製管理情 【課題を解決するための手段】本発明に関する再生装置 報が検出された時に映像または音声情報の再生を停止す る再生制限手段を有することを特徴とする。

20 体に記録された映像または音声情報が所定の暗号方式で 【0009】また、本発明に関する再生装置は、蓄積媒

れていない場合には情報解析手段によって電子透かし情 ハと判定された時にも映像または音声情報の再生を停止 暗号化されていない場合に蓄積媒体に記録された映像ま たは音声情報が電子透かし検出手段において電子透かし 青報を検出できるような正規な映像または音声情報であ 5かどうかを解析する情報解析手段と、薔複媒体に記録 された映像または音声情報が所定の暗号方式で暗号化さ 報を検出できるような正規な映像または音声情報ではな する再生制限手段を有することを特徴とする。

場合に復号した映像または音声情報に重畳されている少 暗号化された入力符号化データを解読してもとの符号化 暗号解読手段を用いず入力符号化データを直接復号する なくとも複製禁止を含む複製管理情報を示す電子透かし 情報を検出する電子透かし検出手段と、暗号解読手段を **引いず入力符号化データを直接復号する場合には電子透** かし検出手段によって何らかの複製管理情報が検出され た時に映像または音声情報の出力を停止する出力制限手 【0010】さらにまた、本発明に関する復号装置は、 された映像または音声情報を復元する暗号解読手段と、 段を有することを特徴とする。

引手段で判別された蓄積媒体の種類および蓄積媒体上の 【0011】さらに、本発明に関する再生装置は、複数 の蓄積媒体の種類および蓄積媒体上の記録フォーマット を判別する媒体およびフォーマット判別手段と、前記複 数の蓄積媒体の種類および蓄積媒体上の記録フォーマッ トそれぞれに定められた暗号方式で暗号化されているか どうかを検出する暗号化検出手段と、蓄積媒体に記録さ **たや映像または音声情報が、媒体およびフォーマット判** 記録フォーマットで定められた暗号方式で暗号化されて いない場合には、電子透かし検出手段の検出結果によっ て何らかの複製管理情報が検出された時に、映像または 育声情報の再生を停止する再生制限手段を有することを

キー交換を行う A K E (Authentication and Key Exchan 出手段と、 AKE手段で認証およびキー交換が成立しな とは音声情報の出力を停止する出力制限手段を有するこ 【0012】また、本発明に関する復号装置は、暗号化 された入力符号化データを解読してもとの符号化された 失像または音声情報を復元する暗号解読手段と、入力符 号化データの供給装置との間の認証と暗号解読に必要な ない状態で復号を開始した時に、復号した映像または音 **声情報に重畳されている少なくとも複製禁止を含む複製** 普理情報を示す電子透かし情報を検出する電子透かし検 ハ状態で復号を開始した時には、電子透かし検出手段に なって何らかの複製管理情報が検出された時に、映像ま ge)手段と、AKE手段で認証およびキー交換が成立し 40

[0013]

【発明の実施の形態】以下、本発明の実施の形態を図面

を用いて詳細に説明する。

【0014】図1は、本発明に係わる再生装置の実施例 路、30は再生制限回路、40は蓄積媒体、50は読み 取り回路、60は再生データ出力端子、150は再生判 て、10は暗号化検出回路、20は電子透かし検出回 の信号の流れを示したプロック図である。図1におい

【0015】本実施例は、DVD-ROMやDVD-R る。読み取り回路50は蓄積媒体40からデータを読み 電子透かし検出回路20及び再生制限回路30へ供給す 取り、読み取った符号化データを暗号化検出回路10、 AMなどの蓄積媒体を再生するいわゆるドライブであ

【0016】例えば、DVD—ROMでは、記録する映 像情報の著作権を保護するため、MPEG2方式で圧縮 符号化された動画像データを暗号化して記録する方式が 用意されており、DVD—RAMでも同様の方式が検討 されている。また、暗号を解いてしまった映像情報に対 しても複製の制限を行うようにするために、複製管理情 報を映像情報上に直接、視聴しても検知できない形で重 これらの暗号化されたり、電子透かしが入れられたりし たDVD―ROMやDVD―RAMを再生することがで 聖する電子透かし方式が検討されている。 本実施例は、

【0017】暗号方式検出回路10は、蓄積媒体40上 に記録された、所定の暗号方式で暗号化されたディスク であることを示す情報を検出する。

【0018】電子透かし検出回路20は、蓄積媒体40 上に記録された映像情報に重量された電子透かしを検出 【0019】再生判定回路150は、条件に応じて、再 ある。暗号化されているディスクの場合は、著作権保護 スクと見なし、再生を停止する。暗号化されていないデ [0020] 図3は、本発明に係わる再生装置の実施例 生データ出力端子60から動画像データを出力するかど 出力する場合には再生データ出力端子60〜動画像デー タを供給し、出力しない場合には再生データ出力端子6 0 ~信号を供給しない。図2は、再生条件を示した図で された正規なディスクなので再生する。暗号化されてい ないディスクの場合で、電子透かし検出回路20により **電子透かしが検出された場合は、遠法に複製されたディ イスクの場合で、電子透かし検出回路20により電子透** かしが検出されなかった場合は、著作権保護されていな いディスクなのでそのまま再生する。これにより、違法 に複製されたディスクの視聴を止めることができ、暗号 化された正規なディスクを再生した時に電子透かしが誤 うかを判定し、再生制限回路30は判定結果に応じて、 **倹出されても誤って再生停止してしまうことがない。** 

の信号の流れを示したプロック図である。図3におい て、10は暗号化検出回路、20は電子透かし検出回

取り回路、60は再生データ出力端子、70は情報解析 回路、150は再生判定回路である。

電子透かし検出回路20、再生制限回路30および情報 [0021] 本実施例も、DVD—ROMやDVD—R る。読み取り回路50は蓄積媒体40からデータを読み 取り、読み取った符号化データを暗号化検出回路10、 AMなどの蓄積媒体を再生するいわゆるドライブであ 解析回路70~供給する。 【0022】暗号方式検出回路10は、蓄積媒体40上 【0023】電子透かし検出回路20は、蓄積媒体40 Lに記録された映像情報に重畳された電子透かしを検出 に記録された、所定の暗号方式で暗号化されたディスク であることを示す情報を検出する。

【0024】情報解析回路70は、電子透かし検出回路 20への入力データが電子透かしの検出回路が可能な正 は、本実施例では、MPEG2方式に合致した正規なデ 規な入力データであるかどうかを解析する。具体的に

された正規なディスクなので再生する。暗号化されてい されていないディスクなのでそのまま再生する。暗号化 より、電子透かしの検出が不能になるように遠法に暗号 【0025】 再生判定回路150は、条件に応じて、再 タを供給し、出力しない場合には再生データ出力端子6 0 ~信号を供給しない。図4は、再生条件を示した図で **ある。暗号化されているディスクの場合は、著作権保護** スクと見なし、再生を停止する。暗号化されていないデ イスクの場合で、電子透かし検出回路20により電子透 出が可能な正規な入力データである場合は、著作権保護 されていないディスクの場合で、電子透かし検出回路2 電子透かしの検出が可能でない不正な入力データである 場合は、電子透かしの検出が不能になるように違法に暗 **号化されたディスクと見なし、再生を停止する。これに** 生データ出力端子60から動画像データを出力するかど 出力する場合には再生データ出力端子60〜動画像デー ないディスクの場合で、電子透かし検出回路20により 電子透かしが検出された場合は、遠法に複製されたディ かしが検出されなかった場合で、かつ、電子透かしの検 うかを判定し、再生制限回路30は判定結果に応じて、 0 により電子透かしが検出されなかった場合で、かつ、 ータであるかどうかを調べる。 40

【0026】図5は、本発明に係わる復号装置の実施例 て、20は電子透かし検出回路、80は暗号解読回路、 90は出力制限回路、100は符号化データ入力端子、 110は暗号解読有無指定入力端子、120は選択回 路、130は復号回路、140は復号データ出力端子、 の信号の流れを示したブロック図である。図5におい 化されたディスクの視聴も止めることができる。

[0027] 本実施例は、MPEG2方式で圧縮符号化 された動画像データを復号するいわゆるデコーダボード 160は出力判定回路である。

-3

20

路、30は再生制限回路、40は蓄積媒体、50は読み

-4-

である。符号化データ入力端子100にはDVD—RO MやDVD一RAMなどの蓄積媒体から再生された符号 化データが入力される。

【0028】本実施例は、暗号化されたDVD—ROM ることができる。暗号解読回路80がこの暗号を解く回 やDVD—RAMから再生される符号化データを復号す

とを指示する信号が入力され、その他の場合には暗号解 【0029】暗号解読有無指定入力端子110には、暗 20は暗号解読する場合には暗号解読回路80で暗号解 タを選択し、復号回路130~供給する。復号回路13 0はMPEG2方式に基づく復号処理を行い、動画像デ **悲しないことを指示する信号が入力される。選択回路1** 読された符号化データを選択し、暗号解読しない場合に ータを復号する。復号された動画像データは復号データ **号化されたディスクを再生する場合には暗号解読するこ** は符号化データ入力端子 100に入力された符号化デ・ 出力端子140から出力される。

[0030] 出力判定回路160は、条件に応じて、復 号データ出力端子140から動画像データを出力するか し検出回路20により電子透かしが検出されなかった場 て、出力する場合には復号データ出力端子140〜動画 端子140~信号を供給しない。図6は、出力条件を示 正規な符号なので出力する。暗号解読しない場合で、電 子透かし検出回路20により電子透かしが検出された場 し、出力を停止する。暗号解読しない場合で、電子透か する。これにより、違法に複製されたディスクからの再 生データの視聴を止めることができ、暗号化された正規 像データを供給し、出力しない場合には復号データ出力 した図である。暗号解読する場合は、著作権保護された 合は、著作権保護されていない符号なのでそのまま再生 なディスクからの再生データを復号した時に電子透かし どうかを判定し、出力制限回路90は判定結果に応じ 合は、違法に複製されたディスクの再生データと見な が誤検出されても誤って出力停止してしまうことがな

しが音声の電子透かしになるだけで、実施例の構成は同 【0031】以上述べた実施例の説明は全て映像情報の **復号化が音声の符号化、復号化になり、映像の電子透か** 場合を説明したが、音声情報の場合も、映像の符号化、 策で、同様の効果が得られる。 [0032] 図7は、複数の種類の蓄積媒体に対応した 再生装置の実施例の信号の流れを示したブロック図であ 図7において、10は暗号化検出回路、20は電子 150は再生判定回路、170は媒体及びフォーマット 体、50は説み取り回路、60は再生データ出力端子、 透かし検出回路、30は再生制限回路、40は蓄積煤

20 [0033] 本実施例は、DVD-ROMとDVD-R AMの複数種類の蓄積媒体を再生するドライブである。

子透かし検出回路20、媒体及びフォーマット判別回路 読み取り回路50は蓄積媒体40からデータを読み取 読み取った符号化データを暗号化検出回路10、 170および再生制限回路30へ供給する。

【0034】 DVD-ROMの画像情報用 (いわゆるD VD-Videoフォーマット)に用意されている暗号 ばれている。DVD—RAMでも同様の方式が検討され 方式は、CSS (Content Scrambling System) 方式と呼 ているが、CSS方式とは異なる暗号方式である。ま

式で圧縮符号化しながら記録するためのリアルタイム記 除フォーマットと、MPEG2方式で圧縮符号化済みの 記録フォーマットがある。ストリーム記録の場合は、圧 **確符号化済みのビットストリームが暗号化された状態で** 送られてくる。リアルタイム記録フォーマットの暗号方 式とストリーム記録フォーマットの暗号方式も、異なる 暗号方式になると予想される。本実施例は、これら全て のディスクおよび暗号方式に対応した再生を行うことが た、DVD—RAMの中でも、画像情報をMPEG2方 ビットストリームをそのまま記録するためのストリーム

【0036】暗号方式検出回路10は、蓄積媒体40の **種類と記録フォーマットに応じて定められた所定の暗号** 【0037】電子透かし検出回路20は、薔獲媒体40 【0035】媒体及びフォーマット判別回路170は、 ち式で暗号化されていることを示す情報を検出する。 **警徴媒体40の種類と記録フォーマットを判別する。** 

20

【0038】再生判定回路150は、条件に応じて、再 うかを判定し、再生制限回路30は判定結果に応じて、

上に記録された映像情報に重畳された電子透かしを検出

タを供給し、出力しない場合には再生データ出力端子6 0~信号を供給しない。図8は、再生条件を示した図で ある。DVD—ROMのVideoフォーマットで暗号 方式がCSS方式の場合は、著作権保護された正規なデ イスクなので再生する。DVD—RAMのリアルタイム マット用暗号方式の場合は、著作権保護された正規なデ イスクなので再生する。DVD—RAMのストリーム記 録フォーマットで暗号方式がストリーム記録フォーマッ ト用暗号方式の場合は、著作権保護された正規なディス クなので再生する。各フォーマットにおいて、暗号化さ れていないディスクの場合で、電子透かし検出回路20 により電子透かしが検出された場合は、違法に複製され たディスクと見なし、再生を停止する。暗号化されてい ないディスクの場合で、電子透かし検出回路20により **電子透かしが検出されなかった場合は、著作権保護され** 生データ出力端子60から動画像データを出力するかど 出力する場合には再生データ出力端子60〜動画像デー 記録フォーマットで暗号方式がリアルタイム記録フォー ていないディスクなのでそのまま再生する。 6

【0039】本実施例によれば、異なる暗号方式が定め

5

る場合にも、違法に複製されたディスクの視聴を止める られた複数種類の記録フォーマットのディスクを再生す ことができ、暗号化された正規なディスクを再生した時 に電子透かしが誤検出されても誤って再生停止してしま

は選択回路、130は復号回路、140は復号データ出 出力制限回路、100は符号化データ入力端子、120 力端子、160は出力判定回路、180はAKE回路で 【0040】図9は、AKE付き復号装置の実施例の信 号の流れを示したブロック図である。図9において、2 0は電子透かし検出回路、80は暗号解読回路、90は

【0041】本実施例は、MPEG2方式で圧縮符号化 である。符号化データ入力端子100にはDVD-RO MやDVD—RAMなどの蓄積媒体から再生された符号 された動画像データを復号するいわゆるデコーダボード 化データが入力される。

外部装置から暗号化された符号化データを受け取って復 取得し、このキーを用いて暗号解読を行う。暗号解読回 【0042】本実施例はAKE回路180を内蔵し、D VD—ROMドライプやDVD—RAMドライプなどの 号する場合には、AKE回路180により外部装置との 間で認証とキー交換 (いわゆるAKE) を行ってキーを 路80がこの暗号を解く回路である。

20

130はMPEG2方式に基づく復号処理を行い、動画 れ、復号が開始された場合には、電子透かし検出回路2 れた動画像データは復号データ出力端子 140から出力 [0043] 選択回路120はAKEが成立して暗号解 読する場合には暗号解説回路80で暗号解読された符号 化データを選択し、AKEが成立せず暗号解読しない場 合には符号化データ入力端子 100に入力された符号化 データを選択し、復号回路130へ供給する。復号回路 像データを復号する。正規なMP E G 2 データが入力さ 0および出力判定回路160~検出信号を送る。復号さ

復号が行われる。

【0044】電子透かし検出回路20は、AKEが成立 せずに復号が開始された場合に、復号された動画像デー タの電子透かしを検出する。

号データ出力端子140から動画像データを出力するか ディスクの再生データと見なし、出力を停止する。AK 【0045】出力判定回路160は、条件に応じて、復 で、復号が動作した場合は、著作権保護された正規な符 合で、復号が動作した場合は、電子透かし検出回路20 により電子透かしが検出された場合、違法に複製された て、出力する場合には復号データ出力端子140〜動画 像データを供給し、出力しない場合には復号データ出力 端子140~信号を供給しない。図10は、出力条件を 号なので出力する。AKEが成立せず暗号解読しない場 示した図である。AKEが成立して暗号解読する場合 どうかを判定し、出力制限回路90は判定結果に応じ

**時開2001-14796** 

9

**合で、電子透かし検出回路20により電子透かしが検出** されなかった場合は、著作権保護されていない符号なの でそのまま出力する。復号が動作しなかった場合は、出 力を停止する。出力しても良いが、復号が動作していな Eが成立せず暗号解読しない場合で、復号が動作した場 いので、この時は意味のある動画像データは出力されな [0046] これにより、AKEの動作しない違法に複 からの再生データを復号した時に電子透かしが誤検出さ 製されたディスクからの再生データの視聴を止めること ができ、AKEが動作する暗号化された正規なディスク れても誤って出力停止してしまうことがない。 10

子透かしがあれば再生を止められるので遠法に複製され 映像または音声情報を再生する再生装置において、所定 の暗号方式で暗号化されていない蓄積媒体については電 た蓄積媒体の視聴を止めることができ、所定の暗号方式 で暗号化されている正規な蓄積媒体については電子透か [発明の効果] 本発明によれば、蓄積媒体に記録された し情報が戦検出されたとしても確実に再生が行われる。

【0048】また、本発明によれば、電子透かし情報が 険出されないように違法な暗号方式で暗号化されている 場合にも再生を止めることができる。

所定の暗号方式で暗号化されていない、符号については電 子透かしがあれば復号を止められるので違法に複製され た蓄積媒体からの符号を復号しての視聴を止めることが でき、所定の暗号方式で暗号化されている正規な符号に ついては電子透かし情報が誤検出されたとしても確実に 【0049】さらにはまた、本発明によれば、符号化さ れた映像または音声情報を復号する復号装置において、

【0050】さらに、本発明によれば、異なる暗号方式 正規な蓄積媒体については電子透かし情報が誤検出され が定められた複数種類の記録フォーマットの蓄積媒体を 再生する場合にも、遠法に複製された蓄積媒体の視聴を 止めることができ、所定の暗号方式で暗号化されている

【0051】また、本発明によれば、AKEの動作した 聴を止めることができ、AKEが動作する正規な符号に い連法に複製された蓄積媒体からの符号を復号しての視 ついては電子透かし情報が誤検出されたとしても確実に たとしても確実に再生が行われる。 40

【図面の簡単な説明】 復号が行われる。

【図1】本発明に係わる再生装置の実施例のブロック

【図2】本発明に係わる再生装置の実施例の再生条件を

【図3】本発明に係わる再生装置の実施例のプロック

【図4】本発明に係わる再生装置の実施例の再生条件を

20

**特開2001-14796** 8

特開2001-14796 6

を示す図。

【図5】本発明に係わる復号装置の実施例のプロック

11

【図6】本発明に係わる復号装置の実施例の出力条件を

【図8】本発明に係わる再生装置の実施例の再生条件を 【図7】本発明に係わる再生装置の実施例のブロック

【図9】本発明に係わる復号装置の実施例のブロック

【図10】本発明に係わる復号装置の実施例の出力条件

図1]

盔

【符号の説明】

0…再生制限回路、40…蓄積媒体、50…読み取り回 80…暗号解読回路、90…出力制限回路、100…符 号化データ入力端子、110…暗号解読有無指定入力端 10…暗号化検出回路、20…電子透かし検出回路、3 子、120…選択回路、130…復号回路、140…復 号データ出力端子、150…再生判定回路、160…出 路、60…再生データ出力端子、70…情報解析回路、 力判定回路、170…媒体及びフォーマット判別回路、 9

180…AKE回路。

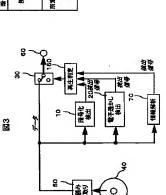
[図3]

ź 19 \$ 編号方式検出 配子透かし核出 された **⊠** f定の方式以外 または 番号集し

[図4]

[図 3]

ร์ ⊠ 4 職号方式校出 電子送かし校出 情 されなかった された f定の方式以外 または 音号無し 所定の方式である



[図 5 <u>図</u>

[ 9 図

[区] <u>M</u>

9 8

 _	
120	4.6
された	きれなかった
Çž	
$\dashv$	\$415

30 60	10 年 150 日本 175	株体および 雑株および 144
	8	

[88]

**8** 

[6|||

0

再生	1.8	งฆา	9.4	
属子説かし 検出	ette ette			
<b>高場方式</b> 数任	CSS 77.5 GL			
195-80	*			
記録媒体	NOG			

	90 140		A M## 20	本部が	15
08 -	100 本語	## 180 ★ 後出	AKE SOHIGH	***	1

[図10] **國** 

れなかった

DVD-RAM

された

끍

43 ន៍ 4.2 49

Ш		1 1	ŧ	-	- S
AKE	動作した動作しない		数作した	数件しない	
網路中田	4.8	#4 Lan		9.4	งสา
ł I	動作した			V 154 1874	
復号 【電子透かし検出】	ı	された	まれなかった		I
出力	4.8	語	48	. 2	Š

ž 4.9

された

ストリーム語

きれなかった

끍

-8-

-7-

5

特開2001-14796

レロントページの結め

种奈川県横浜市戸塚区吉田町292番地 株 式会社日立製作所デジタルメディア開発本 擅 (72) 発明者

GB06 GB11 GB38 HA29 JA03 Fターム(参考) 50053 FA13 FA20 FA21 FA23 GA11

5C063 AA01 AB03 AB05 AC01 AC05 KA21 KA24 LA06

CA11 CA36 DA07

5D044 AB05 AB07 DE49 DE50 EF05 FG18 GK11 GK17 HL08

【発行日】 平成16年11月25日(2004.11.25)

【部門区分】第6部門第4区分

公報種別】特許法第17条の2の規定による補正の掲載

【公開番号】 特開 2001-14796 (P2001-14796A)

[公開日] 平成13年1月19日(2001.1.19)

出願番号】特願平11-233446

[国際特許分類第7版]

5/91 G 1 1 B 20/10 H 0 4 N

1/08 H 0 4 N 7/081 H 0 4 N

20/10

[ F I ]

5/91G 1 1 B H 0 4 N

H P Z

7/08 H 0 4 N

[手統補正書]

[補正対象書類名] 明細書 [手統補正1]

[提出日] 平成15年12月10日(2003.12.10)

【補正対象項目名】特許請求の範

【補正方法】変更

【補正の内容】

【特許請求の範囲】

[請求項1]

蓄積媒体に記録された映像または音声僧報が所定の暗号方式で暗号化されているかどうか を検出する暗号化力式検出手段と、蓄積媒体に記録された映像または音声情報が所定の暗 蓄積媒体に記録された映像または音声情報を再生する再生装置において、

禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と、蓄積媒 透かし検出手段の検出結果によって何らかの複製管理情報が検出された時に映像または音 声情報の再生を複製管理情報に従って制御する再生制限手段を有することを特徴とする再 号方式で暗号化されていない場合に映像または音声情報に重畳されている少なくとも複製 体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合には電子

[請永項2]

生装置。

請求項1に記載の再生装置において、

蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合に <u>、</u>潜額媒体に記録された映像または音声情報が電子透かし検出手段において電子透かし情報を後出できるような正規な映像または音声情報であるかどうかを解析する情報解析手段 を有し、

、情報解析手段によって電子透かし情報を検出できるような正規な映像または音声情報で 蓄積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されていない場合 はないと判定された時に、前記再生制限手段は映像または音声情報の再生を停止する を特徴とする再生装置。

【請永頃3】

符号化された映像または音声情報が入力され、これを復号して映像または音声情報を出力 する復号装置において、

解読指定入力手段と、暗号化された入力符号化データを解読してもとの符号化された映像 入力符号化データが暗号化されているかいないかに従って暗号解読の要・不要を示す暗号

JP 2001-14796 A5 2004.11.25

暗号解読手段からの出力と暗号解読手段を用 とも複製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出手段と いない出力を切り替える選択手段と、切り替え手段から出力された符号化された映像また は音声情報を復号する復号手段と、復号した映像または音声情報に重量されている少なく または音声情報を復元する暗号解読手段と、

暗号解酷手段を用いないで入力された符号化された映像または音声情報を直接復号する場 合には、電子透かし検出手段によって何らかの複製管理情報が検出された時に映像または 音声情報の出力を複製管理情報に従って制御する出力制限手段を有することを特徴とする

[請永項4]

請求項1に記載の再生装置において、

複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットを判別する媒体およびフォ マット判別手段を備え、 前記暗号化力式検出手段は前記複数の蓄積媒体の種類および蓄積媒体上の記録フォーマッ

れた蓄積媒体の種類および蓄積媒体上の記録フォーマットに対応した暗号方式で暗号化さ れていない場合において、前記電子透かし検出手段の検出結果によって何らかの複製管理 情報が検出された時に、再生制限手段は映像または音声情報の再生を複製管理情報に従っ 蓄積媒体に記録された映像または音声情報が、媒体およびフォーマット判別手段で判別 トそれぞれに対応した暗号方式で暗号化されているかどうかを検出する手段であり、 て制御することを特徴とする再生装置。

符号化された映像または音声情報が入力され、これを復号して映像または音声情報を出力 する復号装置において 暗号化された入力符号化データを解読してもとの符号化された映像または音声情報を復元 する暗号解読手段と

入力符号化データの供給装置との間の認証と暗号解読に必要なキー交換を行うAKE手段

暗号解読手段からの出力と暗号解読手段を用いない出力を切り替える選択手段と、

前記選択手段から出力された符号化された映像または音声情報を復号する復号手段と、

AKE手段で認証およびキー交換が成立しない状態で復号を開始した時には、電子透かし 、前記電子透かし検出手段によって何らかの複製管理情報が検出され た時に、映像または音声情報の出力を複製管理情報に従って制御する出力制限手段を有す 号した映像または音声情報に重畳されている少なくとも複製禁止を含む複製管理情報 示す電子透かし情報を検出する電子透かし検出手段とを備え、

ることを特徴とする復号装置。 [請求項6] 蓄積媒体に記録された映像または音声情報を再生する再生方法において

**薔積媒体に記録された映像または音声情報が所定の暗号方式で暗号化されているかどうか** 

前記暗号化方式検出ステップにより蓄積媒体に記録された映像または音声情報が所定の暗 号方式で暗号化されていない場合に、映像または音声情報に重畳されている少なくとも複 製禁止を含む複製管理情報を示す電子透かし情報を検出する電子透かし検出ステップと を検出する暗号化方式検出ステップと、

前記電子透かし検出ステップの検出結果によって何らかの複製管理情報が検出された時に

映像または音声情報の再生を複製管理情報に従って制御する再生制限ステップを有する

とを特徴とする再生方法

水項6に記載の再生方法において

複数の蓄積媒体の種類および蓄積媒体上の記録フォーマットを判別する媒体およびフォー マット判別ステップを備え、 前記暗号化方式検出ステップは前記複数の蓄積媒体の種類および蓄積媒体上の記録フォー

ල

JP 2001-14796 A5 2004, 11, 25

マットそれぞれに対応した暗号方式で暗号化されているかどうかを検出するステップであ

前記媒体およびフォーマット判別ステップで判別された蓄積媒体の種類および蓄積媒体上

の記録フォーマットに対応した暗号方式で暗号化されていない場合には、映像または音声 情報の再生を停止することを特徴とする再生方法。